Google

Using PKI in GPay Soundpod

Presenter : Saurabh Mimani

Overview

- PKI infrastructure gets widely used across GPay to
  - Authenticate users and devices
  - Secure communication channels
  - Maintain integrity of transactions
  - Safeguard data
- We ensure that every interaction within the GPay ecosystem is secure and protected against unauthorized access or manipulation.

Use-cases across GPay

- **Partner ecosystem:** mTLS, PGP based API connectivity
- **Core Payment Flows:** UPI/Card Payments, Tokenization of cards
- **Partner SFTP:** Partner file transfers using key-pairs
- **Google-Wide:** End to end data encryption within and across data-centers (link)
- **GPay Soundpod:** MQTT + mTLS

Google

Pay Soundpod

GPay Soundpod

- Google Soundpod provides comprehensive payment notifications to Google Pay merchants.
- Maintaining merchant trust relies on accurate and timely notifications.
- Soundpod secures its MQTT communication using mTLS.

GPay Soundpod

- Each device is assigned a unique International Mobile Equipment Identity (IMEI).
- Advanced cryptographic standards such as ECDSA (Elliptic Curve Digital Signature Algorithm) and AES (Advanced Encryption Standard) are employed to secure the communication.
- A valid signed device certificate is mandatory for receiving notification from the server.

Device Authentication using PKI

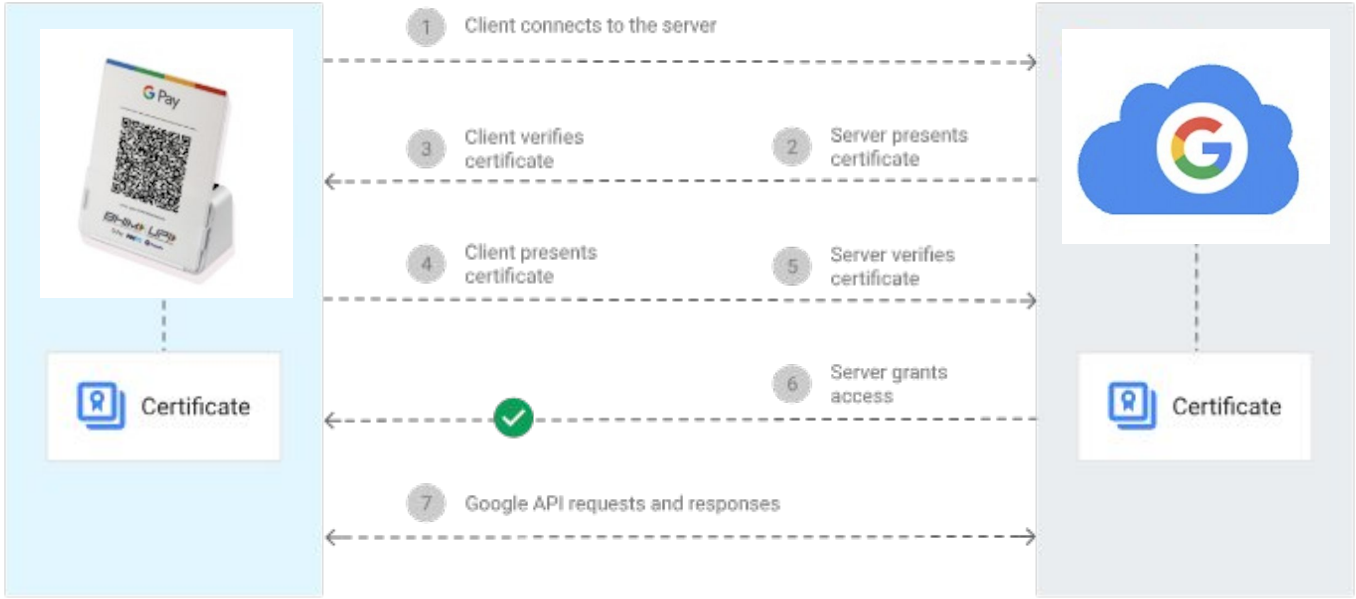
- Devices generate an RSA key pair and a Certificate Signing Request (CSR).
- Root Certificate Authorities (CAs) operating in a secure environment sign the CSRs. The resulting signed certificates(X509), which include the IMEI, are then embedded in the devices.
- Devices are configured with Google server addresses and corresponding certificates.
- Google servers store the root CA certificates that were used to sign the device certificates.

Device Authentication using PKI

To ensure device-server communication security:

- **Mutual Authentication::**
  - Devices verify server identity using embedded certificates.
  - **2-Step auth**:
    - Servers authenticate devices using their certificates, root CA, and embedded IMEI.
    - Client certificates data is used for application-level authentication and authorization.
  - Only allowlisted devices can connect to the mapped topic.

Device Server Handshake (mTLS over MQTT)



Device Authentication using PKI

- **Post-Handshake Protection:**
  - All subsequent communication is encrypted to prevent snooping.
  - mTLS (mutual Transport Layer Security) safeguards against Man-in-the-Middle (MITM) attacks.
  - Device identity bound **authorization** prevents data leak.

Thank You!

Google